PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-308184
(43)Date of publication of application : 05.11.1999

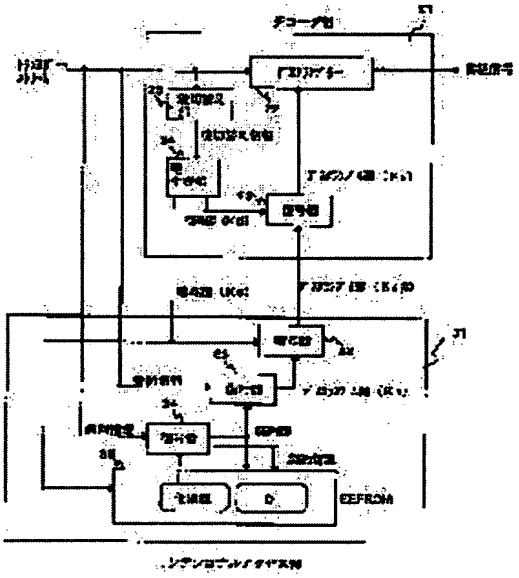
(51)Int.CI. H04H 1/00
H04L 9/08
H04L 9/14
H04N 7/167

(21)Application number : 10-112320
(22)Date of filing : 22.04.1998

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : FUKUDA MASAHIRO

(54) LIMITED RECEIVER AND METHOD THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent the unauthorized use of a limited reception function by allowing decoder to generate a cipher key and a decoding key and decode a ciphered descramble key by using the decoding key, and allowing a conditional access part to cipher the descramble key by using the cipher key from the decoder and give it to a decoder part.
SOLUTION: The conditional access part 31 obtains a contract key and contract information by decoding the individual information of a transport stream in the decoder 34 by using an individual key inside an EEPROM 35 and obtains the descramble key Ks by decoding program information in the decoder 33 by using the contract key. In the meantime, the decoder part 21 generates the cipher key Ke and the decoding key Kd in a key generation part 24. The access part 31 ciphers the descramble key Ks by using the cipher key Ke in a ciphering device 32 and sends the ciphered descramble key Ks# to the decoder part 21. The decoder part 21 decodes the ciphered descramble key Ks# by using the decoding key Kd in the decoder 23 and obtains the descramble key Ks.



LEGAL STATUS

[Date of request for examination] 05.02.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration] abandonment
[Date of final disposal for application] 22.10.2004
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

Citation 2

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－308184

(43)公開日　平成11年(1999)11月５日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｈ	1/00	Ｈ０４Ｈ	1/00	Ｆ
Ｈ０４Ｌ	9/08	Ｈ０４Ｌ	9/00	６０１Ａ
	9/14			６０１Ｅ
Ｈ０４Ｎ	7/167			６４１
		Ｈ０４Ｎ	7/167	Ｚ

審査請求　未請求　請求項の数６　ＯＬ　（全７頁）

(21)出願番号　特願平10－112320

(22)出願日　平成10年(1998)４月22日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　福田　雅裕
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

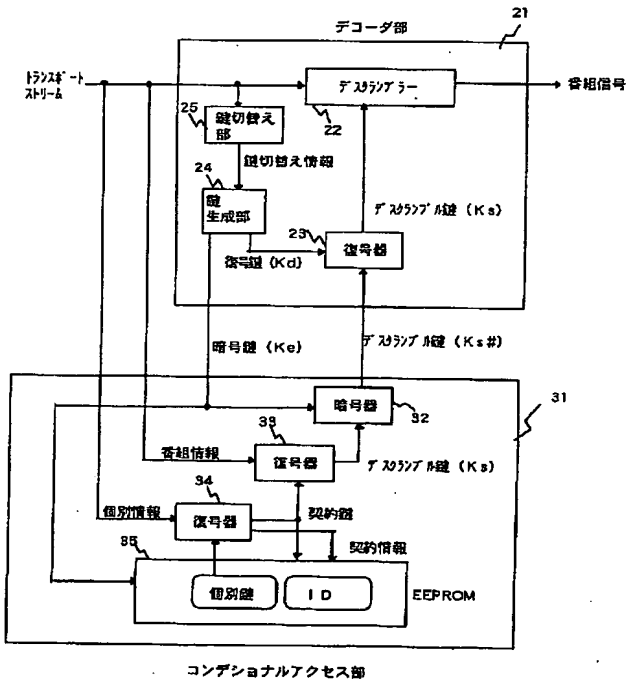
(74)代理人　弁理士　曾我　道照　（外６名）

(54)【発明の名称】　限定受信装置及び方法

(57)【要約】

【課題】　有料デジタル放送において使用されるデスクランブル鍵の不正取得を未然に防ぐことができる限定受信装置及び方法を提供する。

【解決手段】　デコーダ部２１に、暗号鍵をコンデショナルアクセス部３１に与える手段と、コンデショナルアクセス部３１から取得した暗号化されたデスクランブル鍵を復号する手段を備えると共に、コンデショナルアクセス部３１に、デコーダ部２１から取得した暗号鍵を使用して、抽出したデスクランブル鍵を暗号化する暗号手段を備える。



1

【特許請求の範囲】

【請求項１】　放送されてきた複数のトランスポートストリームの中からスクランブルされている所定のトランスポートストリームを選択し、これをデスクランブルするデコーダ部に、

暗号鍵と復号鍵を生成する鍵生成部と、

上記鍵生成部で生成された復号鍵を用いて暗号化されたデスクランブル鍵を復号する復号器と、

上記復号器で復号されたデスクランブル鍵を用いて受信されたトランスポートストリームをデスクランブルして番組信号を得るデスクランブラーとを備えると共に、

上記デスクランブラーで使用するデスクランブル鍵を受信されたトランスポートストリームの中から抽出するコンデショナルアクセス部に、

各視聴者毎に予め配布した個別鍵とＩＤ及び上記鍵生成部で生成された暗号鍵を格納する記憶手段と、

受信したトランスポートストリームから個別情報を抽出して上記記憶手段に格納された個別鍵を用いて個別情報を復号することにより契約鍵及び契約情報を得ると共に、得られた契約情報を上記記憶手段に格納されたＩＤと照合して契約情報に間違いがなければ、得られた契約鍵及び契約情報を上記記憶手段に保持させる第１の復号器と、

受信したトランスポートストリームから番組情報を抽出し、その番組情報を上記第１の復号器で得られた契約鍵を用いて復号して、復号された番組情報からデスクランブル鍵を得る第２の復号器と、

上記鍵生成部で生成された暗号鍵を用いて上記第２の復号器から与えられるデスクランブル鍵を暗号化して暗号化されたデスクランブル鍵を生成して上記デコーダ部に与える暗号器とを備えた限定受信装置。

【請求項２】　請求項１に記載の限定受信装置において、上記鍵生成部は、所定のアルゴリズムに従って複数の暗号鍵と復号鍵の組み合わせの中から一つを選択して上記コンデショナルアクセス部に与える暗号鍵を適時切替えることを特徴とする限定受信装置。

【請求項３】　請求項１に記載の限定受信装置において、上記デコーダ部に、受信されたトランスポートストリームから鍵切り替え情報を抽出する鍵切替え手段をさらに備え、上記鍵生成部は、上記鍵切替え手段からの鍵切替え情報に基づいて複数の暗号鍵と復号鍵の組み合わせの中から一つを選択して上記コンデショナルアクセス部に与える暗号鍵を適時切替えることを特徴とする限定受信装置。

【請求項４】　放送されてきた複数のトランスポートストリームの中からスクランブルされている所定のトランスポートストリームを選択し、これをデスクランブルするデコーダ処理工程として、

暗号鍵と復号鍵を生成し、

生成された復号鍵を用いて暗号化されたデスクランブル鍵を復号し、

2

復号されたデスクランブル鍵を用いて受信されたトランスポートストリームをデスクランブルして番組信号を得ると共に、

上記デコーダ処理工程によりデスクランブルする際に使用するデスクランブル鍵を受信されたトランスポートストリームの中から抽出するコンデショナルアクセス処理工程として、

各視聴者毎に予め配布した個別鍵とＩＤ及び上記生成された暗号鍵を記憶部に格納し、

受信したトランスポートストリームから個別情報を抽出して格納された個別鍵を用いて個別情報を復号することにより契約鍵及び契約情報を得ると共に、得られた契約情報を格納されたＩＤと照合して契約情報に間違いがなければ、得られた契約鍵及び契約情報を上記記憶部に保持させ、

受信したトランスポートストリームから番組情報を抽出し、その番組情報を上記契約鍵を用いて復号して、復号された番組情報からデスクランブル鍵を得、

上記生成された暗号鍵を用いて上記デスクランブル鍵を暗号化して暗号化されたデスクランブル鍵を生成して上記デコーダ処理に与える限定受信方法。

【請求項５】　請求項４に記載の限定受信方法において、上記デコーダ処理工程は、所定のアルゴリズムに従って複数の暗号鍵と復号鍵の組み合わせの中から一つを選択して上記コンデショナルアクセス処理工程に与える暗号鍵を適時切替えることを特徴とする限定受信方法。

【請求項６】　請求項４に記載の限定受信方法において、上記デコーダ処理工程は、受信されたトランスポートストリームから鍵切り替え情報を抽出し、抽出された鍵切替え情報に基づいて複数の暗号鍵と復号鍵の組み合わせの中から一つを選択して上記コンデショナルアクセス処理工程に与える暗号鍵を適時切替えることを特徴とする限定受信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、デジタル放送の受信の際に使用する限定受信装置及び方法に関するものであって、特にデスクランブル鍵の取り扱いに関するものである。

【０００２】

【従来の技術】デジタル放送において放送される番組には、視聴者が放送事業者と契約することによって視聴可能となる有料番組と、契約なしでも視聴可能な無料番組に大別される。この際、有料番組が契約している視聴者のみに視聴可能となるように、放送局では、有料番組の送信時に、有料番組の送信信号にスクランブル処理を施すのが通常である。

【０００３】従って、視聴者が有料番組を視聴するためには、スクランブル処理された有料番組をデスクランブ

ルするためのデスクランブル鍵が必要である。その為に、視聴者は予め放送局に視聴したい番組を連絡し、放送局はその連絡に基づいてデスクランブル鍵を視聴者の受信装置に伝送する。この後、受信装置は、受信したデスクランブル鍵を使ってスクランブル処理された有料番組をデスクランブルすることにより、番組の視聴を可能にする。

【０００４】通常、受信装置は、デジタル放送を受信し、受信信号の復号処理を行うデコーダ部と、前述したデスクランブル鍵の抽出などを行うコンデショナルアクセス部から構成され、コンデショナルアクセス部にて抽出されたデスクランブル鍵は、デコーダ部へ出力されて前述の有料番組のデスクランブル処理に使用される。

【０００５】また、コンデショナルアクセス部は、各視聴者固有の情報を保持していることと、暗号方法の変更にも対応できるように、着脱可能なカードとして実装されることが多い。この際、デスクランブル鍵をそのままの値で、コンデショナルアクセス部とデコーダ部間で受け渡すこととなり、デスクランブル鍵が不正に取得される恐れがでてくる。

【０００６】これを防ぐために、従来、デスクランブル鍵をコンデショナルアクセス部にて暗号化した上でデコーダ部に出力し、デコーダ部にて復号することによりデスクランブル鍵を得る方法が提案されている。このような方法の従来例として、例えば特開平９－４６６７２号公報に開示された「デスクランブル装置および方法」がある。

【０００７】図２は上記公報に開示された従来の限定受信装置を示す構成図である。図２において、２１はデコーダ部、３１はコンデショナルアクセス部であり、デコーダ部２１は、デスクランブラー２２と復号器２３から構成され、コンデショナルアクセス部３１は、暗号器３２、復号器３３、復号器３４、及びＥＥＰＲＯＭ３５から構成される。

【０００８】次に動作について説明する。放送局から受信したデジタル放送信号は、トランスポートストリームとして、デコーダ部２１及びコンデショナルアクセス部３１に入力される。また、コンデショナルアクセス部３１にあるＥＥＰＲＯＭ３５には、各視聴者毎に予め配布した個別鍵とＩＤ（認証番号）が格納されている。受信したトランスポートストリームからは個別情報が抽出され、ＥＥＰＲＯＭ３５内の個別鍵を用いて復号器３４で復号された後、契約鍵及び契約情報が得られる。取り出した契約情報は、ＥＥＰＲＯＭ３５内のＩＤと照合され、契約情報に間違いがなければ、契約鍵及び契約情報はＥＥＰＲＯＭ３５内に保持される。

【０００９】一方、受信したトランスポートストリームからは番組情報も抽出され、この番組情報は前述の契約鍵を用いて復号器３３にて復号され、復号された番組情報からはデスクランブル鍵を得る。このデスクランブル鍵は、暗号器３２により暗号化されて、コンデショナルアクセス部３１からデコーダ部２１に送られる。

【００１０】デコーダ部２１は、この暗号化されたデスクランブル鍵を復号器２３で復号し、デスクランブル鍵を得る。デスクランブラー２１は、復号されたデスクランブル鍵を使用して、トランスポートストリームをデスクランブルし、番組信号を得る。なお、暗号器３２及び復号器２３で使用する暗号鍵及び復号鍵は、ＥＥＰＲＯＭ３５内のＩＤを基にコンデショナルアクセス部３１で生成され、それぞれ暗号器３２及び復号器２３に通知しておく。

【００１１】

【発明が解決しようとする課題】従来の限定受信装置は以上のように構成されており、デスクランブル鍵の復号に用いる復号鍵をそのままの形で、コンデショナルアクセス部３１からデコーダ部２１に伝送するようにしていたので、この復号鍵が不正に取得される恐れがあった。この復号鍵が不正に取得および利用されると、デスクランブル鍵が不正に取得されることとなり、限定受信機能が不正使用されるという問題点があった。

【００１２】この発明は上記のような問題点を解決するためになされたもので、コンデショナルアクセス部からデコーダ部へのデスクランブル鍵の伝送を安全に行い、限定受信機能の不正使用を未然に防ぐことができる限定受信装置及び方法を得ることを目的とする。

【００１３】

【課題を解決するための手段】この発明に係る限定受信装置及び方法は、放送されてきた複数のトランスポートストリームの中からスクランブルされている所定のトランスポートストリームを選択し、これをデスクランブルするデコーダ部に、暗号鍵と復号鍵を生成する鍵生成部と、上記鍵生成部で生成された復号鍵を用いて暗号化されたデスクランブル鍵を復号する復号器と、上記復号器で復号されたデスクランブル鍵を用いて受信されたトランスポートストリームをデスクランブルして番組信号を得るデスクランブラーとを備えると共に、上記デスクランブラーで使用するデスクランブル鍵を受信されたトランスポートストリームの中から抽出するコンデショナルアクセス部に、各視聴者毎に予め配布した個別鍵とＩＤ及び上記鍵生成部で生成された暗号鍵を格納する記憶手段と、受信したトランスポートストリームから個別情報を抽出して上記記憶手段に格納された個別鍵を用いて個別情報を復号することにより契約鍵及び契約情報を得ると共に、得られた契約情報を上記記憶手段に格納されたＩＤと照合して契約情報に間違いがなければ、得られた契約鍵及び契約情報を上記記憶手段に保持させる第１の復号器と、受信したトランスポートストリームから番組情報を抽出し、その番組情報を上記第１の復号器で得られた契約鍵を用いて復号して、復号された番組情報からデスクランブル鍵を得る第２の復号器と、上記鍵生成部

で生成された暗号鍵を用いて上記第２の復号器から与えられるデスクランブル鍵を暗号化して暗号化されたデスクランブル鍵を生成して上記デコーダ部に与える暗号器とを備えたものである。

【００１４】また、上記鍵生成部は、所定のアルゴリズムに従って複数の暗号鍵と復号鍵の組み合わせの中から一つを選択して上記コンデショナルアクセス部に与える暗号鍵を適時切替えることを特徴とするものである。

【００１５】また、上記デコーダ部に、受信されたトランスポートストリームから鍵切り替え情報を抽出する鍵切替え手段をさらに備え、上記鍵生成部は、上記鍵切替え手段からの鍵切替え情報に基づいて複数の暗号鍵と復号鍵の組み合わせの中から一つを選択して上記コンデショナルアクセス部に与える暗号鍵を適時切替えることを特徴とするものである。

【００１６】また、この発明に係る限定受信方法は、放送されてきた複数のトランスポートストリームの中からスクランブルされている所定のトランスポートストリームを選択し、これをデスクランブルするデコーダ処理工程として、暗号鍵と復号鍵を生成し、生成された復号鍵を用いて暗号化されたデスクランブル鍵を復号し、復号されたデスクランブル鍵を用いて受信されたトランスポートストリームをデスクランブルして番組信号を得ると共に、上記デコーダ処理工程によりデスクランブルする際に使用するデスクランブル鍵を受信されたトランスポートストリームの中から抽出するコンデショナルアクセス処理工程として、各視聴者毎に予め配布した個別鍵とＩＤ及び上記生成された暗号鍵を記憶部に格納し、受信したトランスポートストリームから個別情報を抽出して格納された個別鍵を用いて個別情報を復号することにより契約鍵及び契約情報を得ると共に、得られた契約情報を格納されたＩＤと照合して契約情報に間違いがなければ、得られた契約鍵及び契約情報を上記記憶部に保持させ、受信したトランスポートストリームから番組情報を抽出し、その番組情報を上記契約鍵を用いて復号して、復号された番組情報からデスクランブル鍵を得、上記生成された暗号鍵を用いて上記デスクランブル鍵を暗号化して暗号化されたデスクランブル鍵を生成して上記デコーダ処理に与えるものである。

【００１７】また、上記デコーダ処理工程は、所定のアルゴリズムに従って複数の暗号鍵と復号鍵の組み合わせの中から一つを選択して上記コンデショナルアクセス処理工程に与える暗号鍵を適時切替えることを特徴とするものである。

【００１８】さらに、上記デコーダ処理工程は、受信されたトランスポートストリームから鍵切り替え情報を抽出し、抽出された鍵切替え情報に基づいて複数の暗号鍵と復号鍵の組み合わせの中から一つを選択して上記コンデショナルアクセス処理工程に与える暗号鍵を適時切替えることを特徴とするものである。

【００１９】

【発明の実施の形態】図１はこの発明の限定受信装置及び方法を説明するための構成図である。図１において、２１はデコーダ部、３１はコンデショナルアクセス部である。デコーダ部２１において、２２はデスクランブラー、２３は復号器、２４は鍵生成部、２５は鍵切替え部である。また、コンデショナルアクセス部３１において、３２は暗号器、３３は復号器、３４は復号器、３５はＥＥＰＲＯＭである。

【００２０】次に動作について説明する。放送局から受信したデジタル放送信号として、複数のトランスポートストリームの中からスクランブルされている所定のトランスポートストリームを選択され、デコーダ部２１及びコンデショナルアクセス部３１に入力される。また、コンデショナルアクセス部３１にあるＥＥＰＲＯＭ３５には、各視聴者毎に予め配布した個別鍵とＩＤ（認証番号）が格納されている。

【００２１】コンデショナルアクセス部３１においては、受信したトランスポートストリームから個別情報を抽出し、ＥＥＰＲＯＭ３５内の個別鍵を用いて復号器３４で個別情報を復号した後、契約鍵及び契約情報が得られる。取り出した契約情報は、ＥＥＰＲＯＭ３５内のＩＤと照合され、契約情報に間違いがなければ、契約鍵及び契約情報は、ＥＥＰＲＯＭ３５内に保持される。一方、受信したトランスポートストリームからは番組情報も抽出され、この番組情報は、前述した契約鍵を用いて復号器３３にて復号され、復号された番組情報からはデスクランブル鍵（Ｋｓ）を得る。

【００２２】一方、デコーダ部２１では、鍵生成部２４が暗号鍵（Ｋｅ）と復号鍵（Ｋｄ）を生成する。暗号の方法としては、公開鍵暗号を使用し、公開鍵を暗号鍵（Ｋｅ）とし、秘密鍵を復号鍵（Ｋｄ）とする。また、暗号鍵（Ｋｅ）と復号鍵（Ｋｄ）は、予めデコーダ部２１に組み込まれたものであり、復号鍵（Ｋｄ）については外部からは読み出すことができないようにデコーダ部２１内で厳重に保持されている。鍵生成部２４は、生成した暗号鍵（Ｋｅ）を暗号器３２に出力すると共に、ＥＥＰＲＯＭ３５に格納する。

【００２３】暗号鍵（Ｋｅ）は公開鍵であるので不正に取得されても問題はない。前述の契約鍵、契約情報及び暗号鍵（Ｋｅ）をＥＥＰＲＯＭ３５に格納することにより、電源投入毎にデコーダ部２１の鍵生成部２４から暗号鍵（Ｋｅ）を読み出す必要がなく、迅速な視聴が可能となる。

【００２４】暗号器３２は、この暗号鍵（Ｋｅ）を使ってデスクランブル鍵（Ｋｓ）を暗号化し、暗号化されたデスクランブル鍵（Ｋｓ＃）を生成する。デスクランブル鍵（Ｋｓ＃）は、コンデショナルアクセス部３１からデコーダ部２１に送られ、デコーダ部２１内の復号器２３が、鍵生成部２４から取得した復号鍵（Ｋｄ）を使用

して、暗号化されたデスクランブル鍵（Ｋｓ＃）を復号し、デスクランブル鍵（Ｋｓ）を得る。

【００２５】デスクランブラー２２は、復号されたデスクランブル鍵（Ｋｓ）を使用して、トランスポートストリームをデスクランブルし、番組信号を得る。

【００２６】また、鍵生成部２４は、暗号鍵（Ｋｅ）と復号鍵（Ｋｄ）の生成に際しては、デコーダ部２１に組み込まれた複数の暗号鍵（Ｋｅ）と復号鍵（Ｋｄ）の組み合わせの中から一つを所定のアルゴリズムに従って適時選択するようにすることもできる。また、デコーダ部２１内の鍵切替え部２５が、受信したトランスポートストリームから鍵切替え情報を抽出して、この情報に基づいて鍵生成部２４が使用する暗号鍵（Ｋｅ）と復号鍵（Ｋｄ）を選択するようにしてもよい。

【００２７】以上のように、コンデショナルアクセス部３１とデコーダ部２１間でのデスクランブル鍵の伝達における暗号鍵及び復号鍵をデコーダ部２１内の鍵生成部２４において公開鍵方法に基づて生成するようにしたので、デスクランブル鍵を不正に取得されることを防止することができ、より安全性の高い限定受信装置を得ることができる。

【００２８】

【発明の効果】以上のように、本発明の限定受信装置及び方法によれば、コンデショナルアクセス部及び処理工程とデコーダ部及び処理工程間でのデスクランブル鍵の伝達における暗号鍵及び復号鍵を公開鍵方法に基づて生成するようにしたので、デスクランブル鍵を有料放送を契約していない人が不正に取得することを防ぐことができる為、デジタル放送における安全性の高い有料放送を実施することが可能となる。

【００２９】また、暗号鍵と復号鍵の生成に際しては、デコーダ部及び処理工程に組み込まれた複数の暗号鍵と復号鍵の組み合わせの中から一つを所定のアルゴリズムに従って適時選択するようにし、または、デコーダ部及び処理工程で、受信したトランスポートストリームから鍵切替え情報を抽出して、その情報に基づいて使用する暗号鍵と復号鍵を選択するようにしたので、適時選択して変えるすることでデスクランブル鍵の不正取得を防止するのにさらに安全性を高めることができる。

【図面の簡単な説明】

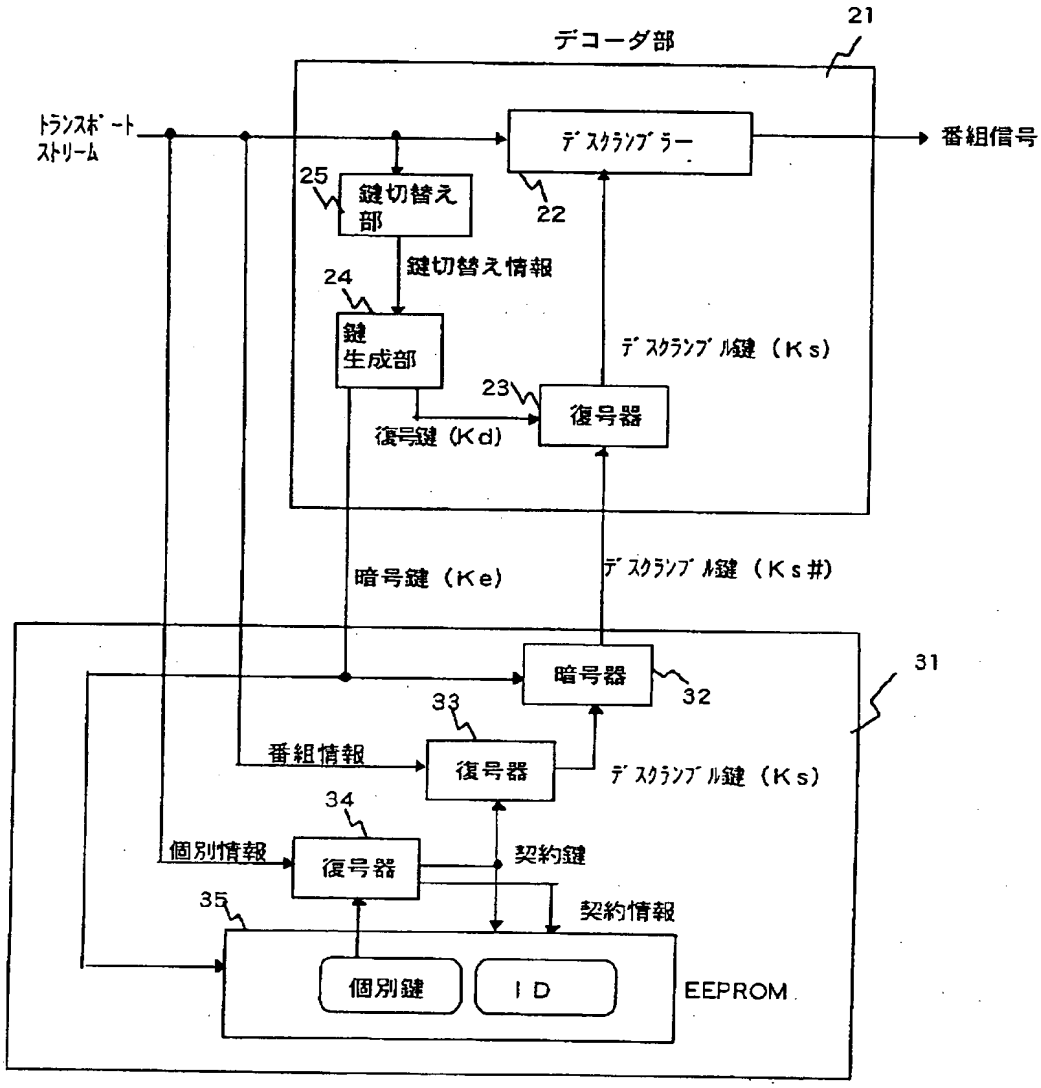
【図１】　この発明の限定受信装置及び方法を説明するのに用いた構成を示すブロック図である。

【図２】　従来の限定受信装置の構成を示すブロック図である。

【符号の説明】

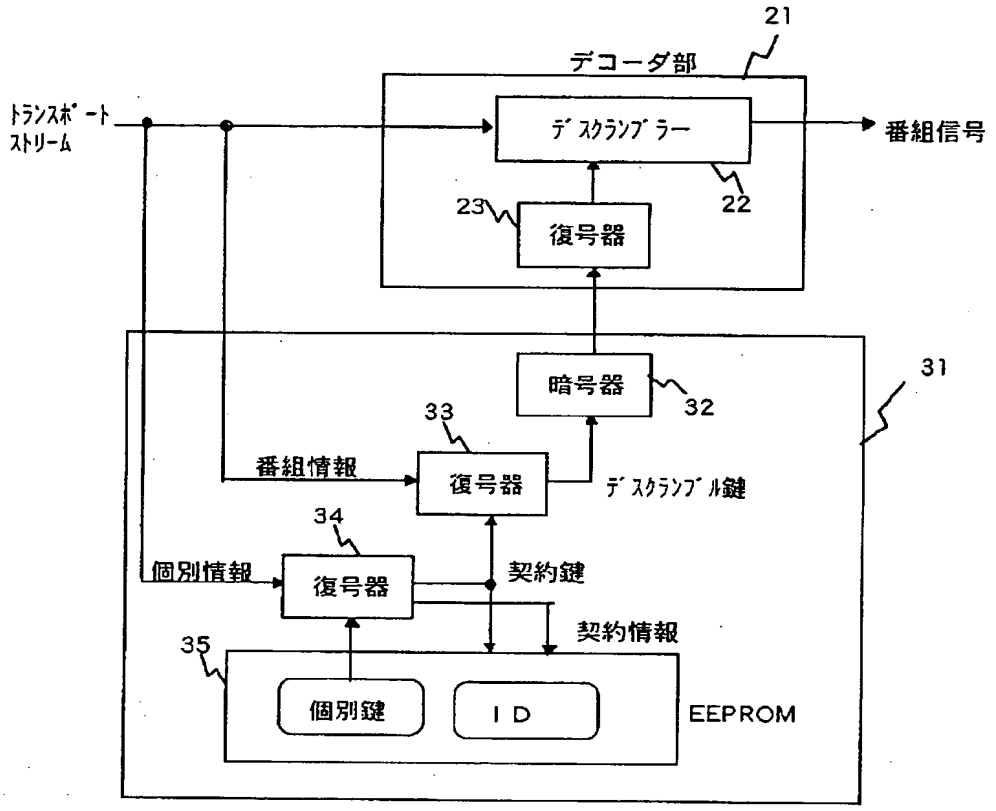
２１　デコーダ部、２２　デスクランブラー、２３　復号器、２４　鍵生成部、２５　鍵切替え部、３１　コンデショナルアクセス部、３２　暗号器、３３　復号器、３４　復号器、３５　ＥＥＰＲＯＭ。

【図１】



コンデショナルアクセス部

【図２】



コンデショナルアクセス部